| | |
|---|---|
| **From:** | Richard Tontodonato |
| **To:** | Steven Stokes; Matt Forsbacka |
| **Subject:** | FW: DOE hack by Anonymous |
| **Date:** | Tuesday, February 05, 2013 8:18:00 AM |
| **Attachments:** | image001.png<br>image002.png<br>image004.png |

Dr. Mansfield included Kupferer on his distribution but not you guys

**From:** John Mansfield
**Sent:** Tuesday, February 05, 2013 8:14 AM
**To:** Jeremy Bingham; Michael Leggett; Joseph Bader; David Kupferer; jmansfie@post.harvard.edu; Jessie Roberson; Sean Sullivan; Timothy Dwyer; Peter Winokur; Dave Jonas; Jessie Roberson; John Mansfield; Richard Tontodonato; Rick Schapira
**Subject:** DOE hack by Anonymous

Energy Department networks hit by sophisticated cyber attack

Credit: DOE Website

BY: Bill Gertz
February 4, 2013 5:00 am

Computer networks at the Energy Department were attacked by sophisticated hackers in a major cyber incident two weeks ago and personal information on several hundred employees was compromised by the intruders.

Energy Department officials, along with FBI agents, are investigating the attack on servers at the Washington headquarters. They believe the sophisticated penetration attack was not limited to stealing personal information. There are indications the attackers had other motives, possibly including plans to gain future access to classified and other sensitive information.

No classified information was compromised in the cyber attack, said officials who provided details of the attack to the Washington Free Beacon on condition of anonymity.

Energy Department and FBI spokesmen declined to comment.

The source or identity of the cyber attacker is not known, according to U.S. officials and outside security analysts. However, Chinese hackers are likely suspects because the department is known to be a major target of China for both secrets and technology. Also, the relative sophistication of the cyber attack is an indication of nation-state involvement.

The department's National Nuclear Security Administration is in charge of developing and maintaining U.S. nuclear weapons and related infrastructure.

Spies successfully targeted those systems for decades. The U.S. government revealed in the 1990s that espionage by China resulted in the compromise of secrets related to all deployed nuclear weapon in the U.S. arsenal in crimes that remain unsolved.

The cyber attack was confirmed Friday by DOE security officials and is still under investigation. Officials are working to determine the exact nature of the attack and the extent of potential damage.

The personal data compromised involves information related to several hundred people, the officials said.

A total of 14 computer servers and 20 workstations at the headquarters were penetrated during the attack.

The department is currently in the process of notifying the employees and contractors whose information was stolen.

The department is planning steps to plug security holes in its network that were revealed by the attack, the officials said.

Efforts also are underway to prevent future attacks through increased monitoring of networks and the use of specialized cyber defense tools, they said.

The compromised data is "personally identifiable information" that can be used by criminals or foreign intelligence services for illicit purposes, in information security terms.

The U.S. government defines this type of information as: full name; national identification number, such as a Social Security number; Internet Protocol addresses; vehicle and driver's license numbers; face, fingerprint or handwriting samples; credit card numbers; digital identity; date of birth; birthplace; and genetic information.

Hackers are known to steal and use such information for what is called "doxing"—from documents or ".docx"—in furtherance of targeting people for exposure or additional theft operations.

Foreign intelligence agencies would use such information to obtain further details of targets for

agent recruitment or additional cyber espionage.

Ed McCallum, who spent 10 years as the Department of Energy's Office of Safeguards and Security, said the latest security breach highlights decades of poor security at the department.

"It's a continuing story of negligence," McCallum, now a security consultant, told the Free Beacon.

The department "is on the cutting edge of some of the most sophisticated military and intelligence technology the country owns and it is being treated frivolously by the Department of Energy and its political masters," McCallum said.

McCallum said the Chinese have been targeting DoE for a long time and now the Iranians are beginning to try and steal DoE secrets.

"A lot of countries are interested in our secrets and unless security is improved, this is going to happen again," he said.

An Energy official said all headquarters employees were notified in an email on Friday of what the notice said was "a recent cyber incident."

The security breach "resulted in the unauthorized disclosure of employee and contractor Personally Identifiable Information (PII)" of several hundred people, the email stated.

"The Department is strongly committed to protecting the integrity of each employee's PII and takes any cyber incident very seriously," the email said. "The Department's Cybersecurity Team, the Office of Health, Safety and Security and the Inspector General's office are working with federal law enforcement to promptly gather detailed information on the nature and scope of the incident and assess the potential impacts to DOE staff and contractors."

The email added that "based on the findings of this investigation, no classified data was compromised."

Employees were urged to use encryption for all files and emails containing sensitive information, including data stored on hard drives and shared on networks. Also, storing or emailing non-government personal information from Energy network computers was discouraged.

Disclosure of the Energy Department computer hack comes as the New York Times, Wall Street Journal, and Washington Post reported this week they were victims of Chinese cyber attacks.

The Times stated in a report that its computer networks were compromised around the time the newspaper exposed extensive corruption last fall by then-Chinese Premier Wen Jiabao.

Twitter, the online social media outlet, also reported on Friday that data related to 250,000 of its 250 million users had been compromised. That breach was detected as it occurred, according to computer security specialists familiar with details of the attack.

A report by the U.S. China Economic and Security Review Commission made public in November stated that "U.S. industry and a range of government and military targets face repeated exploitation attempts by Chinese hackers, as do international organizations and nongovernmental groups including Chinese dissident groups, activists, religious organizations, rights groups, and media institutions."

"In 2012, Chinese state-sponsored actors continued to exploit U.S. government, military, industrial, and nongovernmental computer systems," the report said.

Attributing individual cyber attacks is difficult "but security researchers are increasingly able to group exploitations into 'campaigns' based on common features and gain better insight into those

responsible," the report said.

The report said Chinese cyber exploitation capabilities last year were "improving significantly."

"Irrespective of sophistication, the volume of exploitation attempts yielded enough successful breaches to make China the most threatening actor in cyberspace," the congressional commission report said.

China is also modernizing its nuclear arsenal and thus could be seeking weapons and related information from Department of Energy networks.

"Chinese actors are the world's most active and persistent perpetrators of economic espionage," according to a 2011 report by the U.S. government's Office of the National Counterintelligence Executive. The report said U.S. intelligence agencies expect China to remain one of the most "aggressive and capable collectors of sensitive US economic information and technologies, particularly in cyberspace."

The Chinese, as well as the Russians, "will almost certainly continue to deploy significant resources and a wide array of tactics to acquire this information from US sources, motivated by the desire to achieve economic, strategic, and military parity with the United States," the report said.

China is seeking to continue its policy of "catching up fast and surpassing" Western powers, including a secret program called Project 863 that "provides funding and guidance for efforts to clandestinely acquire US technology and sensitive economic information."

Specifically, the Chinese are "more aggressively" targeting U.S. "clean" energy-generating technologies, the report said.

The Energy Department is known to be developing such technologies.

China's military has been targeting U.S. government computer networks for at least a decade, including both military and civilian government systems.

A 2011 Pentagon report on China's military stated that cyberwarfare capabilities support military operations in three areas.

"First and foremost, they allow data collection through exfiltration," the report said. "Second, they can be employed to constrain an adversary's actions or slow response time by targeting network-based logistics, communications, and commercial activities. Third, they can serve as a force multiplier when coupled with kinetic attacks during times of crisis or conflict."

A computer forensic expert who specializes in investigating hacking attacks said an anti-nuclear weapons and anti-Israel group linked to Anonymous that calls itself by the Twitter hashtag #Parastoo may be linked to the attack. Parastoo was suspected of an earlier hacker attack on networks of the International Atomic Energy Agency in November.

A Jan. 21 notice by the group posted on a hacker web site stated "PARASTOO IS SPEAKING." It called for "serious investigations" of Israeli nuclear facilities.

"To show you *a glance* of how serious and active #Parastoo is, we hearby publish part of information about of the USA Department of Energy critical services we have access to," the posting stated, adding that it may publish more of the pilfered data in the future.

"We also have access to your 'access,'" it stated in explaining some of the stolen computer code posted on Pastebin.

The computer forensic specialist said the data disclosed by the group reveals "they were firmly into

the network they compromised."

The posting was signed using the Anonymous manifesto, which begins "We are Anonymous."

However, a U.S. source said the Jan. 21 posting contained information that was dated and thus investigators believe Anonymous is less likely behind the attack.

This entry was posted in China and tagged China, Department of Energy, hackers. Bookmark the permalink.